



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/540,613	03/31/2000	Carl M. Ellison	042390.P8628	2175

8791 7590 04/04/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN  
12400 WILSHIRE BOULEVARD  
SEVENTH FLOOR  
LOS ANGELES, CA 90025-1030

EXAMINER

TRAN, ELLEN C

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 04/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/540,613

Applicant(s)

ELLISON ET AL.

Examiner

Ellen C Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 05 November 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 61-94 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 61-94 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date Nov 2004/ Jan 2005.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

***DETAILED ACTION***

1. This action is responsive to communication: 5 November 2004, with an original filing date of 31 March 2000.
2. Claims 1-60 have been canceled by amendment. Claims 61-94 have been added.
3. Claims 61-94 are currently pending in this application. Claims 61, 72, and 84 are independent claims. The amendment to the claims and specification is accepted.

***Response to Arguments***

4. Applicant's arguments with respect to anticipated rejection have been considered but are not persuasive.

With respect to applicant's first argument on page 14, "Carloganu has nothing to do with a processing system that supports "isolated execution mode" and "normal execution mode". The Office disagrees see '749 col. 2, lines 35-67. In this passage Carloganu explains the procedures for operating a set of control resources under the control a secure processor. Also in the passage Carloganu states: "command primitive associated with the command code in each of the secured commands is then executed if and only if" this passage has the same meaning as an isolated execution mode.

With respect to applicant's argument on page 14, "In addition, the independent and dependent claims recite numerous additional features that are not disclosed by Carloganu. For example, claim 76 recites the operation of "storing a thread count" to indicate "a number of threads operating in the isolated execution mode...and claim 74 recites the operation of obtaining at least part of the PE handler from "PE handler storage" in a chipset of the processing system". The Office disagrees Carloganu these features see col. 8, lines 40-67 "For example, in

an embodiment in which command sequence is required to be sequential and the security module itself tracks the Nxt\_Seq\_ID, the command sequence ID can be encrypted as part of the step of preparing an application software program. When decrypted in the security module as part of secured command processing routine 51, the secured command is simultaneously authenticated and checks as to sequence, i.e. if the Seq\_ID for current command, tracked in the security module, matches the expected Nxt\_Seq\_ID which is generally part of the previous secured command". The tracking of the Seq\_ID has the same meaning as "thread count". In addition, the "security module" and "expected Nxt\_Seq\_ID" has the same meaning as "PE handler storage".

***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

6. Claims 61-94 are rejected under 35 U.S.C. 102(e) as being anticipated by Carloganu et al. U.S. Patent No. 6,226,749 (hereinafter '749).

As to independent claim 61, "A processing system comprising: a processor to support an isolated execution mode, a normal execution mode, a first privilege ring within the normal execution mode for use by an operating system (OS) kernel, and a second privilege ring within

Art Unit: 2134

the normal execution mode for use by a software application” is taught in ‘749 col. 3, lines 30-59;

“a memory responsive to the processor, the memory to include an isolated memory area, the isolated memory area to be inaccessible to the processor in the normal execution mode” is shown in ‘749 col. 10, lines 12-26;

“a chipset responsive to the processor, the chipset to support the normal execution mode and the isolated execution mode” is disclosed in ‘740 col. 21, lines 10-45;

“processor executive (PE) handler storage in the chipset to store at least part of a PE handler, the PE handler to be loaded into the isolated memory area during a boot process for the processing system after at least a portion of the processing system is initialized, the PE handler to manage, from the isolated execution mode, at least one subsequent operation in the boot process” is taught in ‘749 col. 7, lines 32-61.

As to dependent claim 62, “wherein the processing system enters the isolated execution mode before loading the PE handler into the isolated memory area” is shown in ‘749 col. 7, lines 32-61.

As to dependent claim 63, “further comprising: a thread count storage, the processing system to store, in the thread count storage, a thread count indicating a number of threads operating in the isolated execution mode” is disclosed in ‘749 col. 8, lines 40-52.

As to dependent claim 64, “further comprising: an initialization storage, the processing system to update the thread count in response to access to the initialization storage” is taught in ‘749 col. 8, lines 16-67.

As to dependent claim 65, “wherein the processing system provides indication of a failure mode in response to the thread count reaching a thread limit” is shown in ‘749 col. 8, lines 1-15.

As to dependent claim 66, “further comprising: a log storage to store identifiers of executive entities operating in the isolated execution mode” is disclosed in ‘749 col. 8, lines 16-38.

As to dependent claim 67, “further comprising: key storage to store a key to be used to handle one or more executive entities to operate in the isolated execution mode” is shown in ‘749 col. 5, line 65 through col. 6, line 18.

As to dependent claim 68, “wherein the key comprises data based on a substantially random value generated by a manufacture of hardware for the processing system” is disclosed in ‘749 col. 5, line 65 through col. 6, line 18.

As to dependent claim 69, “further comprising: storage responsive to the processor; and at least one executive entity encoded in the storage, the at least one executive entity selected from the group consisting of a processor executive (PE) and an operating system executive (OCS), the at least one executive entity to operate in the isolated execution mode” is taught in ‘749 col. 10, lines 12-25.

As to dependent claim 70, “further comprising: configuration storage to store a base value and a mask value, the processing system to establish the isolated memory area in the memory based at least in part on the base value and the mask value” is shown in ‘749 col. 9, lines 20-56.

As to dependent claim 71, “wherein the PE handler storage comprises substantially non-volatile storage” is disclosed in ‘749 col. 7, lines 43-61.

As to independent claim 72, A method comprising: initializing a processing system during a boot process for the processing system” is taught in ‘749 col. 9, lines 40-56;

“wherein the processing system comprises a processor and a memory, the processing system to support an isolated execution mode, a normal execution mode, a first privilege ring within the normal execution mode for use by an operating system (OS) kernel, and a second privilege ring within the normal execution mode for use by a software application” is shown in ‘749 col. 3, lines 30-59;

“during the boot process, establishing an isolated memory area in the memory, the isolated memory area to be inaccessible from the normal execution mode” is disclosed in ‘749 col. 10, lines 12-36;

“and after at least a portion of the processing system is initialized, loading a processor executive (PE) handler into the isolated memory area, the PE handler to manage, from the isolated execution mode, at least one subsequent operation in the boot process” is taught in ‘col. 9, lines 40-56.

As to dependent claim 73, wherein the processing system further comprises a chipset with a PE handler storage, the method further comprising: obtaining at least part of the PE handler from the PE handler storage of the chipset” is shown in ‘749 col. 21, lines 10-45. As to dependent claim 74, “wherein the PE handler storage comprises substantially non-volatile storage” is disclosed in ‘749 col. 7, lines 43-61.

As to dependent claim 75, “further comprising: entering the isolated execution mode before loading the PE handler into the isolated memory area” is taught in ‘749 col. 7, lines 32-61.

As to dependent claim 76, “wherein the processing system further comprises a thread count storage, the method further comprising: storing a thread count in the thread count storage, the thread count indicating a number of threads operating in the isolated execution mode” is shown in ‘749 col. 8, lines 40-52.

As to dependent claim 77, “further comprising: providing indication of a failure mode in response to the thread count reaching a thread limit” is disclosed in ‘749 col. 8, lines 1-15.

As to dependent claim 78, “wherein the processing system further comprises an initialization storage, the method further comprising: updating the thread count in response to access to the initialization storage” is shown in ‘749 col. 8, lines 16-67.

As to dependent claim 79, “further comprising: operating one or more executive entities in the isolated execution mode; and storing identifiers of the executive entities operating in the isolated execution mode” is disclosed in ‘749 col. 8, lines 16-38.

As to dependent claim 80, “wherein the processing system comprises key storage to store a key, the method further comprising: using the key to handle one or more executive entities to operate in the isolated execution mode” is taught in ‘749 col. 5, line 65 through col. 6, line 18.

As to dependent claim 81, “wherein the key comprises data based on a substantially random value generated by a manufacture of hardware for the processing system” is shown in ‘749 col. 5, line 65 through col. 6, line 18.

As to dependent claim 82, “further comprising operating one or more executive entities in the isolated execution mode, wherein the executive entities comprise at least one entity selected from the group consisting of a processor executive (PE) and an operating system executive (OSE)” is disclosed in ‘749 col. 3, lines 30-59.



As to dependent claim 83, wherein the processing system comprises configuration storage to store a base value and a mask value, and the operation of establishing an isolated memory area in the memory comprises: using the base value and the mask value to establish the isolated memory area” is taught in ‘749 col. 9, lines 20-56.

As to independent claim 84, this claim is direct to an apparatus of the method of claim 61; therefore it is rejected along similar rationale.

As to dependent claims 85-94, these claims contain substantially similar subject matter as claim 62-70; therefore they are rejected along similar rationale.

### ***Conclusion***

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

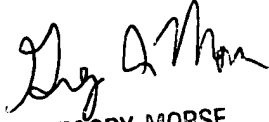
Art Unit: 2134

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system; see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen. Tran  
Patent Examiner  
Technology Center 2134  
18 March 2005

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2134